Ministerstwo Cyfryzacji

PWCyber

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Departament Cyberbezpieczeństwa

SZKOLENIE ONLINE DLA PODMIOTÓW KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

17 lutego 2026 r.
Typ 200
AI a Cyberbezpieczeństwo w przyszłości – Trendy i Kierunki
ENGAVE

9.45 – 10.00	**Logowanie**
10.00 – 10.05	**Zasady organizacyjne przebiegu szkolenia** *Przedstawiciel Departamentu Cyberbezpieczeństwa MC*
10.05 – 12.00	**Wstęp i fundamenty** • Ewolucja zagrożeń • Dual-use AI • Obalenie mitów • Zmiana paradygmatu **Ofensywne wykorzystanie AI – Czego się bać?** • Deepfakes 2.0 i Voice Cloning • Automatyzacja exploitów • Hyper-personalized Phishing • Zatruwanie danych (Data Poisoning) **Defensywne AI – Jak się bronić?** • Self-healing networks & Predictive Analytics • AI w SOC (Security Operations Center) • Weryfikacja tożsamości • Walka maszyn **Zagrożenia wewnętrzne i przyszłość** • Wyścig zbrojeń • Regulacje i etyka • Shadow AI

Rekomendacje i najlepsze praktyki

- Audyt Shadow AI
- Polityka bezpieczeństwa (Acceptable Use Policy)
- Uwierzytelnianie
- Procedura "Safe Word"

Ekspert „ENGAVE": Paweł Kacprzak
Ekspert „ENGAVE": dr inż. Jarosław Wilk

12.00 – 12.10 **Sesja pytań i odpowiedzi do ekspertów**